Network Security Lab – Cryptography

Srinivas Piskala Ganesh Babu – spg349 & N13138339

Network Security Laboratory CS 6823

NetID: spg349

1. RSA

a. Computing the Public (n,e) and Private Key (n,d)

i. Prime Numbers **p=13** and **q=3**

ii. Compute **n = pq** = 13 * 3 = 39

PHI = (p-1)(q-1) = 12 * 2 = 24

iii. Select **e < PHI** (such that they are relatively PRIME)

Possible values of e = 5,7,11,13..

Selecting small value e = 5

iv. Compute **ed mod PHI = 1** (to calculate d)

5d mod 24 =1

- Method 1:
  a. 5 * 5 mod 24 = 25mod24 = 1
- Method 2:
  a. Let (5d -1)/24 = k
  Then, **d = (24k + 1)/5**
  b. Select k =1 gives d = 5

v. Therefore the Public Key is **(n,e) = (39, 5)**

And the Private Key is **(n,d) = (39, 5)**

b. Last Two Digits of NYU ID = **49**

Message = 49 mod 38 = 11

Encrypt Message **= m^e mod n** = 11 ^ 5 mod 39 = 20

- 11^1 mod 39 = 11
- 11^2 mod 39 = (11^1mod39*11^1mod39)mod39 = 11 * 11 mod 39=4
- 11^5 mod 39 = (11^2mod39*11^2mod39*11^1mod39)mod39
  = 4*4*11 mod 39 = 20

Decrypt Message = **20^d mod n =** 20 ^ 5 mod 39 = 11

- 20^1 mod 39 = 20
- 20^2 mod 39 = 20*20mod39 = 10
- 20^3 mod 39 = (20^2mod39*20^1mod39)mod39 = 20*10 mod 39 = 5
- 20^5 mod 39 = (20^3mod39*20^2mod39)mod39 = 5*10 mod 39 = 11

2. Diffi-Helman:

a. Net ID – 49
therefore, Alice **choice a = 14**
Bob choice b **= 19**

b. g = 3; n = 11;

c. Alice computation: **A = g^a mod n** = 3^14 mod 11 = 4

- 3^1 mod 11 = 3
- 3^2 mod 11 = (3^1mod11*3^1mod11)mod11 = 9
- 3^4 mod 11 = 9*9 mod 11 = 4
- 3^8 mod 11 = 4*4 mod 11 = 5
- 3^14 mod 11 = ((3^8mod11)*(3^4mod11)*(3^2mod 11)mod11) = 5*4*9 mod 11 = 4

Bob computation: **B = g^b mod n** = 3^19 mod 11 = 4

- 3^19 mod 11 = (3^14mod11*3^4mod11*3^1mod11) mod11 = 4*4*3 mod 11 = 48mod11 = 4

d. Alice Computation: **Key = B^a mod n** = 4^14 mod 11 = **3**

- 4^1 mod 11 = 4
- 4^2 mod 11 = 4*4 mod 11 = 5
- 4^3 mod 11 = 5*4 mod 11 = 9
- 4^6 mod 11 = (4^3mod11*4^3mod11)mod11 = 4

- 4^12 mod 11 = 4*4mod11 = 5
- 4^14 mod 11 = (4^12mod11*4^2mod11)mod11 = 5*5 mod 11 = 3

Bob Computation**: Key = A^b mod n** = 4^19 mod 11 = **3**

- 4^19 mod 11 = ((4^14mod11)*(4^3mod11)*(4^2mod11)mod11) = 3*9*5 mod 11 = 3

Both the Keys Match, hence the calculation is correct.